REMARKS

Applicants respectfully request reconsideration of the present application in view of the foregoing amendments and in view of the reasons that follow.

Claim 42 has been amended.

This amendment changes claims in this application. A detailed listing of all claims that are, or were, in the application, irrespective of whether the claim(s) remain under examination in the application, is presented, with an appropriate defined status identifier.

After amending the claims as set forth above, claims 42-56 are now pending in this application.

Claim Rejections under 35 U.S.C. § 103

Claims 42-56 were rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,745,574 ("Muftic") in view of U.S. Patent Publication No. 2002/0031230 ("Sweet et al.") and in further view of Alfred J. Menezes et al., *Handbook of Applied Cryptography*, CRC Press, 1997 ("Menezes et al."). In response, Applicants amend independent claim 42 and respectfully traverse the rejection for the reasons set forth below.

Applicants rely on M.P.E.P. § 2143, which states that to establish a prima facie case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation in the prior art to modify the reference. Second, there must be a reasonable expectation of success. Third, the prior art must teach or suggest all the claim limitations. Applicants submit that none of the references, alone or in combination, discloses each and every element of independent claim 42.

In the embodiment of claim 42, the method of communicating credentials comprises communicating a composite credential to a second party. The composite credential comprises a plurality of obfuscated credentials. Different obfuscation is used for at least two credentials in the composite credential. The second party de-obfuscates at least one credential. In addition, the second party communicates to a third party at least one obfuscated credential from the composite credential wherein the third party obtains a credential of the first party from the obfuscated credential without directly communicating with the first party.

In contrast, the combination of Muftic, Sweet and Menezes et al. do not disclose, teach or suggest each and every limitation of independent claim 42 as amended. Muftic is directed to a security infrastructure for electronic transactions. Sweet is directed toward security management using a web-based application service model. Finally, Menezes et al. is a text book on general cryptography.

The Menezes et al. reference relied on by the Examiner defines a "trusted third party" as "an entity in the network which is trusted by all other entities." (*See* Menezes et al. at 36.) Menezes et al. discloses that if two entities (A_1 and A_5) wish to communicate with each other, the trusted third party must generate a session key to facilitate communication between A_1 and A_5. (*See* FIG. 1.16). The trusted third party sends the session key to both A_1 and A_5. Then as shown in FIG. 1.16, A_5 obtains the credentials of A_1 by communicating directly with A_1.

Further, the Office Action states that "Menezes teaches a certificate may come from a user/trusted third party, (page 39, 1.11.3)." Applicants disagree. Menezes et al. only states that a trusted third party "may have access to the secret and private keys of users." Menezes et al. does not disclose, teach or suggest that the trusted third party communicates the secret or private keys to other users. Access to user keys does not imply the ability to communicate those user keys to other parties. Moreover, support for the assertion that a certificate may come from a user/trusted third party is simply not present in Menezes et al.

Accordingly, Menezes et al. does not disclose, teach or suggest a method of communicating credentials wherein the second party communicates to a third party at least one obfuscated credential from the composite credential wherein the third party obtains a credential of the first party from the obfuscated credential without directly communicating with the first party. The communications between the first and third party as claimed do not require the steps of (1) establishing an initial interaction with a "trusted third party" and then (2) conducting direct communication between the first and third parties as taught in Menezes et al. Thus, because of the composite credentials, direct communication between the first party and third party claimed in claim 42 is unnecessary. Accordingly, Applicants respectfully submit that the combination of Muftic, Sweet and Menezes fails to teach each and every element of claim 42 and request that the rejection be withdrawn.

In addition, claims 43-56 depend from independent claim 42 as amended and should be allowed for at least the reasons set forth above. Accordingly, Applicant respectfully requests that the rejection be withdrawn and claims 43-56 be allowed.

Conclusion

Applicants believe that the present application is now in condition for allowance. Favorable reconsideration of the application as amended is respectfully requested.

The Examiner is invited to contact the undersigned by telephone if it is felt that a telephone interview would advance the prosecution of the present application.

At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account 08-2025 pursuant to 37 C.F.R. § 1.25. Additionally, charge any fees to Deposit Account 08-2025 under 37 C.F.R. § 1.16 through § 1.21 inclusive, and any other sections in Title 37 of the Code of Federal Regulations that may regulate fees.

Respectfully submitted,

Date 11/21/06

By W. Keith Robinson Reg No 59,396

/for/ William T. Ellis
Registration No. 26,874

Walter Keith Robinson
Registration No. 59,396

HEWLETT-PACKARD COMPANY
Customer No.: 22879
Telephone: (202) 672-5485
Facsimile: (202) 672-5399